

---

# Cryptography

---

## Encryption

---



Harald Greifensteiner  
Technology Consulting

All Rights Reserved



## Inhalt:

### **1. Einleitung**

### **2. Public Key Kryptographie**

- 2.1. Einführung
- 2.2. Authentication
- 2.3. Integrity
- 2.4. Vergleich Secret Key – Public Key
  - 2.4.1. Encryption Speed
  - 2.4.2. Key Länge
  - 2.4.3. Key Distribution
  - 2.4.4. Symmetrischer Key
  - 2.4.5. Asymmetrischer Key

### **3. Distribution von Public Keys**

- 3.1. Digital Certificates
- 3.2. X.509 Public Key Infrastructure (PKI)
  - 3.2.1. Certificate Management
  - 3.2.2. Certificate Authority (CA)
  - 3.2.3. X.509 Trust Network
  - 3.2.4. X.509 Certificate Data
- 3.3. Vergleich PGP (Pretty good Privacy) versus X.509 Certificates

### **4. Secure E-Mail**

### **5. Secure Socket Layer (SSL) und Transport Layer Security (TLS)**

### **6. IPsec**

- 6.1. Key Management
- 6.2. User Authentication und Key Exchange unter Verwendung von IKE
- 6.3. Bulk Data Confidentiality und Integrity
  - 6.3.1. ESP + Transport Mode
  - 6.3.2. ESP + Tunnel Mode
  - 6.3.3. AH + Transport Mode
  - 6.3.4. AH + Tunnel Mode

### **7. Public Key Algorithmen**

- 7.1. RSA
- 7.2. Diffie- Hellman
- 7.3. DSA
- 7.4. Elliptic Curve Cryptography (EEC)
  - 7.4.1. EC Diffie-Hellman
  - 7.4.2. EC DAS

### **8. Ciphers**

- 8.1. DES
- 8.2. Triple DES
- 8.3. Blowfish
- 8.4. AES / Rijndael